REMARKS

Claims 1-20 are pending in the application. The Non-Final Office Action dated October 19, 2005, has rejected Claims 1-20. Claims 1, 3, 5, and 8 are objected to because of informalities. Also, the specification is objected to for informalities.

Claim 14 is amended to correct a typographical error. Claims 1, 3, 5, and 8 are amended to correct informalities. The specification is amended to correct an incorrect reference to a figure number. Additionally, Claim 1 and 13 are amended to further clarify the claimed invention. No new matter has been added by any of these amendments. For at least the reasons discussed below, the pending claims are patentable over the art of record.

Objections to the Specification

The Specification has been objected to for referring to the wrong figure number. In response, the reference number for "General Packet Radio Service Nodes (GGSNs)" has been amended to $135_{\text{A-B,}}$ instead of $125_{\text{A-B}}$.

Objections to Claims 1, 3, 5, and 8

The Office Action noted that the articles in Claim 1 are inappropriate. Claim 1 is amended to read "an MN", "an FA", and "an HA." Additionally, for Claims 1 and 5, the misspelling of "Diffie-Helman" has been amended to read "Diffie-Hellman." Also, a change in verb tense was made for Claim 3, i.e., "includes" is amended to read "include." Lastly, for Claim 8, the term "fail" is changed to read "failure." Therefore, for at least these reasons, amended Claims 1, 3, 5, and 8 are now no longer objectionable and allowable.

Rejections under 35 U.S.C. § 112

Claims 1-12 are rejected under 35 U.S.C. § 112 as being indefinite. Claim 1, prior to an amendment, states "an FA is configured to: … authenticate, decrypt, sign and send the Reg-Reply message to the MN." The Office Action objects to the recitation of decrypting the Reg-Reply messages because originally Claim 1 did not mention encrypting this message. Claims 2-12 were rejected because they depend on Claim 1.

However, Claim 1 is now amended to clarify that it is the session keys that are decrypted, not the Reg-Reply message. At least for this reason, amended Claim 1 is in now condition for allowance. Also, since Claims 2-12 depend from amended Claim 1, they are in condition for allowance for substantially similar reasons as Claim 1.

Rejections of Claims 1-3 and 12-15 under 35 U.S.C. § 103(a)

Claims 1-3 and 13-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Igarashi et al. (U.S. Patent No. 09/783,185, hereinafter Igarashi) in view of Faccin et al. (U.S. Patent Application No. 2002/0118674, hereinafter Faccin) and in further view of Borella et al. (U.S. Patent No. 6,948,074, hereinafter Borella).

Igarashi is generally directed towards a system for distributing from a foreign agent (FA) to a mobile node (MN), information about a service provided by a network. Igarashi Abstract. The Office Action suggests that Igarashi's system architecture is similar to the system of Claim 1 in that it includes an AAAF and an AAAH node which authenticate messages according to the AAA protocol, a home agent (HA) node, and an FA node. Office Action, p.4, para 5. The Office Action suggests that the nodes of Igarashi and Claim 1 transmit registration-request (Reg-Req) and registration-reply (Reg-Reply) messages in a similar manner. Id. Igarashi also teaches the use of security information in messages from the AAAF node. Igarashi, p. 13, para 267-269. Faccin is directed to a method for exchanging Diffie-Hellman keys between network nodes. Faccin Abstract. Borella is directed towards the distributed generation of unique random numbers, and teaches the authorization of messages using X.509 public/private key authentication. Borella Abstract.

Unfortunately, the Office Action did not appreciate the differences in the functionality between Igarashi's nodes and the nodes as claimed in Claim 1, or the differences between Igarashi's messages and the messages claimed by Claims 1 and 13. In particular, the Office Action does not take into account the large differences in the use of session keys by the claimed invention and the cited references.

Briefly, amended Claim 1 recites, among other things, "an MN that is configured to: … receive a Reg-Reply message that includes session keys that may be used to directly communicate with the AAAH, AAAF, HA, and FA nodes while the MN is in a foreign authority," and "an AAAH that is configured to: receive and authenticate the Reg-Req message; generate a second at least one key of the session keys; sign and send the Reg-Req message; receive and authenticate the Reg-Reply message; generate a third at least one key of the session keys; encrypt the session keys; sign and send the Reg-Reply message to the AAAF." Claim 1, emphasis added.

Amended Claim 1 is not made obvious by Igarashi in view of Faccin and Borella, because it utilizes more than one session key, and the session keys are also generated by at least the *AAAH*. In contrast, in Igarashi, the system "obtain[s] *a* session key from the *AAAF*." Igarashi, page 14, paragraph 267, emphasis added. Furthermore, in Claim 1, the session keys included in the Reg-Reply message are received by the MN, whereas in Igarashi, the session key is only used by the FA node, and no mention is made of sending session keys to the MN. Igarashi, p. 13, para 267-269. The use of multiple session keys allows an MN "to directly communicate with the AAAH, AAAF, HA, and FA nodes." In contrast, Igarashi does not disclose that the MN is enabled to communicate directly to the AAAH, AAAF, HA or FA nodes. See Igarashi, Figure 1 (MN 11 is connected only to FA 5). Clearly, the single session key of Igarashi cannot perform the same functions enabled by the session keys of amended Claim 1. Therefore, for at least these reasons, amended Claim 1 is not made obvious by Igarashi in view of Faccin and in further view of Borella.

Similar to amended Claim 1, amended Claim 13 recites "creating a plurality of session keys by the AAAH and the AAAF." For at last substantially similar reasons discussed above, Igarashi does not disclose the use of multiple session keys as recited in amended Claim 13. Therefore, Igarashi in view of Faccin and in further view of Borella does not make obvious amended Claim 13.

Furthermore, Claims 2 and 3 depend from amended Claim 1, and are allowable for at least the same reasons as Claim 1. Also, Claims 14 and 15 depend from amended Claim 13 and they allowable are for at least the same reasons too.

Moreover, nothing in Borella suggests that its distributed generation of random numbers could be combined with the mobile service discovery system taught by Igarashi. Absence some suggestion or teaching, the Office Action cannot pick and choose disparate elements of references to find claims obvious. Additionally, neither Faccin or Igarashi suggests that an AAAH could generate the session keys. Accordingly, Claims 1-3 and 13-15 are now in condition for allowance at least in view of the discussion presented above.

Rejections of Claims 4-12 and 16-20 under 35 U.S.C. § 103(a)

Claims 4-12 and 16-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Igarashi in view of Faccin in further view of Borella, and further in view of Dowling (U.S. Patent Application No. 2002/0062385).

Dowling is directed to a method and system that allows mobile devices to wirelessly contract for products and services. Dowling Abstract. Dowling teaches the use of security associations to digitally sign messages sent between nodes. Dowling, p. 13, para 116.

The Office Action argues that Igarashi in view of Faccin teaches the use of security associations to authenticate messages between nodes, but does not expressly mention the signing of messages by the security associations. The Office Action reasons that Igarashi in view of Faccin can be combined with the security associations usage of Dowling to make obvious the teachings of Claim 4.

However, Dowling doesn't suggest that it can be combined with the Igarashi system in view of Faccin. It is noteworthy that Dowling does not teach the claimed nodes, i.e., AAAH, AAAF, HA, or FA. See Dowling, Figure 1. Thus, there can be no suggestion that Dowling can be combined with the protocols between the nodes as disclosed in Igarashi. See Dowling, Figure 5, and 6. Additionally, as discussed above, Igarashi in view of Faccin does not make obvious amended Claim 1 upon which Claim 4 depends. Therefore, Claim 4 is also non-obvious for at least this reason.

Claims 5-12 depend either directly or indirectly on Claim 4. In regard to Claim 9, Dowling mentions a negotiation module but does not teach or suggest that the negotiation module is "configured to protect the authentication process from a replay attack." Dowling, page 4, paragraph 43.

In contrast, Claim 9 recites that "the AAH is further configured to protect the authentication process from a replay attack." In regard to Claim 10, the Office Action suggests that the Igarashi's "service profile" functions in the same way as the security associations of Claim 10. Igarashi, page 8, paragraphs 173-176. However, Igarashi does not mention that the service profile performs the functions of a security association. Thus, Igarashi in view of Faccin, in further view of Borella, and in further view of Dowling can not make obvious the novel aspects of Claims 5-12.

Additionally, Claim 16 is rejected for substantially similar reasons as Claim 4. Also, Claims 17-20 depend either directly or indirectly from Claim 16. Therefore, Claim 16 should be allowable for substantially similar reasons as presented above for Claim 4. Moreover, Claims 17-20 are in condition for allowance for at least the same reasons as Claim 16, upon which they depend.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: January 19, 2006

Respectfully submitted,

By____________________
John W. Branch
Registration No.: 41,633
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8900
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant